DOCUMENT RESUME

ED 321 737 IR 014 499

AUTHOR Friedman, Batya
TITLE Moral Responsibility and Computer Technology.
PUB DATE Apr 90
NOTE 11p.; Paper presented at the Annual Meeting of the American Educational Research Association (Boston, MA, April 16-20, 1990).
PUB TYPE Viewpoints (120) -- Speeches/Conference Papers (150)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS *Computer Software; *Copyrights; Elementary Secondary Education; Higher Education; *Intellectual Property; *Microcomputers; *Moral Values
IDENTIFIERS *Computer Crimes; *Computer Piracy; Computer Security

ABSTRACT

Noting a recent increase in the number of cases of computer crime and computer piracy, this paper takes up the question, "How can understanding the social context of computing help us--as parents, educators, and members of government and industry--to educate young people to become morally responsible members of an electronic information community?" Four central characteristics of computer innovations are identified that may contribute to the difficulty of responsible computer use: increased physical and temporal distance of the actor to the consequences of a computer-mediated action, the delegation of decision making to the computer, the initial absence of pervasive social conventions governing computer use, and cultural inexperience with technological innovation. Drawing on this analysis, parameters for an educational approach to promote responsible computer use are outlined. It is argued that such an approach must: (1) make visible (as opposed to hiding) the consequences of computer-mediated actions; (2) help students understand that people control the use of technology (including where and for what purposes technology is used); (3) help students to identify and clarify the conventional aspects of computer use; and (4) stimulate students to develop a watchful eye for unanticipated consequences or abuses of computer use. The paper concludes with a brief description of a strategy for applying these guidelines in the classroom using student self-governance to resolve many of the social issues that concern their use of computers. (19 references) (GL)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

X This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

Moral Responsibility and Computer Technology

Batya Friedman

Mills College

Paper presented in W. F. Arsenio (Chair), Educating for moral responsibility across societal contexts, symposium conducted at the April 1990 annual meeting of the American Educational Research Association, Boston.

Author's address: Director, Interdisciplinary Computer Science Graduate Program, Mills College, 5000 MacArthur Blvd., Oakland, CA 94613.

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Batya Friedman

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

BEST COPY AVAILABLE

ED321737

IR014499

Moral Responsibility and Computer Technology

This past year when word of viral epidemics, anti-viral precautions, and disinfectants filled the press, chances are that personal computers and not people were the sick ones under discussion (Doig, 1989; Elmer-De Witt, 1988). Equally eventful in the news have been stories of computer spies and hackers who gain unauthorized access to the computer systems belonging to banks, hospitals, and the military (Clark & Schneidawind, 1989; "Computer," 1990), and stories of computer pirates who routinely make unauthorized copies of commercial computer programs (DiNucci, 1985; Taylor, 1986). These types of activities usually represent irresponsible use of electronic information and computer technology. Moreover, given that young people appear to participate as perpetrators in these types of activities to a disproportionately high degree (see Bloombecker, 1986; Parker, 1984), I wish today to take up the following question: How can understanding the social context of computing help us -- as parents, educators, and members of government and industry -- to educate young people to become morally responsible members of an electronic information community. Specifically, I shall point to characteristics of computer use that make it especially difficult to promote responsible computing. Then, based on this analysis, I shall offer some modest teaching suggestions.

To begin, picking up a thread from Peter's talk, when Martin Buber (1947/1965) says, "Genuine responsibility exists only where there is real responding," Buber continues by asking, "Responding to what?" and answers, "To what happens to one, to what is to be seen and heard and felt" (pg. 16). Thus, for Buber responsibility depends in some real sense on what happens about and within oneself, on what one hears, sees, and feels. As a quick

illustration, consider again the Kitty Genovese example: If someone in the apartment building heard no cries or heard only vague unusual night noises, then would that person be responsible to come to Kitty Genovese's aid? In this particular case I think not, though one might still feel remorse at not having heard or heard clearly enough and thus not being able (response-able) to act.

To a certain extent, a psychological counterpart to Buber's point can be found in Milgram's study (1974) which highlights the role of proximity of the agent to the victim, that is the clarity with which an individual can hear, see, and know another's plight -- in that individual's moral judgments and actions. In brief, Milgram found that the more remote the potential victim from the agent, the more likely the agent was to cause the victim "harm." Milgram offers several psychological factors that may explain this finding. Let me slightly recast three that are particularly relevant to a discussion of computer-mediated action. First, with remote interactions the agent may have less knowledge of the harm caused to the victim and what knowledge the agent has is inferred rather than directly apprehended. Second, the remoteness of the victim may make it easier for the agent to put the victim out of mind. And third, when the victim does not know the agent, the agent may feel less accountable to the victim.

Consider these factors then in the common instance of pirating computer programs: Pirating a piece of commercial software in the quiet of one's home feels very different from stealthily taking a physical copy of the same software off a store shelf under the eyes of the shopkeeper who will suffer the loss of the merchandise. In the case of pirating, it is difficult to identify a "real" loss of property as no tangible property is taken. Moreover, the programmer, the most readily identifiable individual negatively affected

by the act, is not present at the time of pirating so is easily "out of mind," nor is the software pirate likely ever to meet the programmer face-to-face.[1,2]

In addition to the distancing effects of computer-mediated actions, delegating decision making to a computer further complicates the difficulty of assessing moral responsibility with computer use. For in such situations of, say, launch on warning missile detection systems or automated patient monitoring systems it may be difficult if not impossible to determine who or what is causally responsible for poor if not disastrous computer decisions. That is, if we cannot identify an agent, where do we place blame? With the computer program? the computer programmer? the computer operator? the administration? In the face of this complexity, it is tempting to retreat to a position such as that implied by Snapper (1985), that questions of accountability cannot be answered and, thus, from a pragmatic viewpoint are useless to ask.

---

[1] A further complexity of remote computer use not anticipated in Milgram's study concerns the potential for the victim to be unaware or only vaguely aware that he or she has been harmed. For example, with computer pirating the computer programmer may never learn of the act and hence never know that a "theft" occurred -- that is, never know that he or she had suffered a loss. Or if the programmer suspects a loss, then it is only diffuse and unspecific.

[2] Considering moral obligation, the distancing effect for computer-mediated actions calls into question the extent to which we are morally obligated to sensitize ourselves to overcome this effect -- to actively seek to hear, see, feel, and know better the circumstances. Correspondingly, returning to the Kitty Genovese example, if one knows that rapes and murders regularly occur in one's neighborhood, to what extent is one obligated to listen more carefully?

Both characteristics of computer use that I have discussed thus far -- the distancing of the agent from consequences and the delegation of decision making to computers -- are in some sense material characteristics of computer use.[1] For example, whether I am sending a message to an electronic bulletin board for the first time or for the thousandth time, I am engaged in an activity which distances me from the consequences of my immediate actions.

In contrast, other characteristics of computer use that additionally contribute to the difficulty of assuming responsibility stem from the computer's status in terms of cultural convention (Turiel, 1983). Since computers comprise a relatively recent innovation, the initial absence of agreed upon and pervasive social conventions can make it difficult to know how to fit the new technology into the on-going web of human activities. For instance, consider information stored on electronic media in a "computer" file. For the first computer file, how is one to know whether to consider this electronic information as private or public information? Should the information be thought of as akin to a personal paper file or to a public message on a bulletin board (as was the case with some of the first computer systems, such as that at the MIT Artificial Intelligence Lab)? Clearly, there is no a priori correct view of electronic information as private or public information. What privacy status makes sense for electronic information will depend minimally on shared expectations pertaining to the type of information included, and to who uses the information and for what

---

[1] Granted, over time, an individual engaging in such activities is likely to gain experience and information that affects how he or she thinks about the computer use; however, the fundamental character of the computer use remains unchanged.

purposes. Such shared understandings and conventions to govern computer use evolve in society over time.

For young people, the absence of well established conventions can be confusing. Some students may interpret this absence to mean that anything goes. More likely, as my own research suggests (Friedman, 1988, 1989), students struggle to arrive at some coherent set of conventions that makes sense for the situation in which they experience computer use. For example, because teachers look at students' computer files to evaluate their work and because students work on the same assignments on school computers, some students may come to the conclusion that students do not put private information on school computers. Other students, however, may use a word processor to write private letters or use other software for other personal work and, thus, construct an understanding that computer files are private. In the absence of well articulated and pervasive conventions to govern students' privacy expectations for their school computer use, students with different expectations can come into conflict. So too, may be the case with some young computer enthusiasts who understand computer hacking (e.g., breaking the password to another's computer file) as akin to ferreting out someone's unlisted phone number and not as akin to picking the lock on someone's front door.

Finally, our culture's inexperience with the technology can affect what counts as negligent use of the technology. As an illustration, consider the recent computer worm invented and unleashed into a national computer network by 24 year-old Robert Morris. According to the Associated Press (Kates, 1990), Morris claimed to be experimenting with a new sort of computational entity, a computer worm -- a piece of computer code that replicates itself. The experiment, however, went out of control. "Morris said

he thought the computer worm would duplicate a few times a day or every few hours. Instead, the worm spread 'far faster than I expected.'...'I couldn't control it'." To determine irresponsible computer use we are left with the following questions: If we believe Morris that the program's consequences were legitimately unanticipated, has Morris acted in a negligent manner? To what extent does the computing community's lack of experience with such programs affect what we judge as negligence or irresponsibility in this instance?

To summarize, thus far I have identified four central characteristics of computer innovations which may contribute to the difficulty of responsible computer use. These characteristics include: the increased physical and temporal distance of the actor to the consequences of a computer-mediated action, the delegation of decision making to the computer, the initial absence of pervasive social conventions governing computer use, and cultural inexperience with technological innovation.

Drawing on this analysis, we can now begin to identify parameters for an educational approach to promote responsible computer use.[1] An

---

[1] While this paper focuses on educational approaches to the problem of promoting responsible computing, other approaches may be found by rethinking the material conditions established by the technology. That is, we can design technology that better supports responsible use. For example, in certain situations it may be feasible for expert systems to recommend two or three reasonable courses of action (rather than a single "best" course) and, thereby, assure the final decision for a course of action rests with the individual using the technology. Yaakov discusses the latter type of approach in terms of responsibility and the environment in his paper that follows.

educational approach must make visible (as opposed to hide) the consequences of computer-mediated actions. The approach must help students understand that people control the use of technology, including determining where and for what purposes technology is used. The approach must help students to identify and clarify the conventional aspects of computer use. Finally, the approach must stimulate students to develop a watchful eye for unanticipated consequences or abuses of computer use.

I do not have time to describe what one can actually do in the classroom based on these approaches. If interested, I would be pleased to send you two papers of mine that work out these approaches in some depth (see Friedman, 1986, 1989). But let me leave you with a brief sense of one overarching strategy I have used with students from elementary to graduate school. This overarching strategy builds on Kohlberg's just community work (1980, 1985) by using student self-governance to resolve many of the social issues that concern students' own computer use -- issues such as resource allocation, privacy of student computer files, ownership of student computer programs, and management of student electronic bulletin boards. Said succinctly, students determine, implement, and monitor policies that govern their own school computer use. Because of the largely self-contained nature of classrooms, when violations of student-generated policies occur, the consequences of those computer-mediated actions for others are likely to be more visible as the "victims" are likely to be classmates. Moreover, in the course of establishing and fine-tuning student generated policies, students come to realize that people determine how and for what computer technologies are used. Through this, the goal is for students to realize and take seriously that people (themselves included) are responsible for computer use.

References

Bloombecker, J. (1986). Computer crime, computer security, computer ethics: The first annual statistical report of the National Center for Computer Crime Data. Los Angeles, CA: The National Center for Computer Crime Data.

Buber, M. (1965). Between man and man. New York: The Macmillan Company. (Original work published 1947)

Clark, D. & Schneidawind, J. (1989, November 2). Tracking down a spy through a computer maze. San Francisco Chronicle, p. C3.

Computer workers charged. (1990, January 19). Sun Sentinel, p. A3.

DiNucci, D. (1985, September). Copying software: Who's right? PC World, pp. 126-130, 134-139.

Doig, S. K. (1989, November 12). Quiet viruses wait to strike in computers. Miami Herald.

Elmer-De Witt, P. (1988, September 26). Invasion of the data snatchers! Time Magazine, pp. 62-67.

Friedman, B. (1986, October). If I only had one more computer... Facing the sticky issues of resource allocation. Classroom Computer Learning, pp. 44-45.

Friedman, B. (1988, April). Adolescents' conceptions of computer piracy: An analysis of social-cognition in the context of technological change. Paper presented at the meeting of the American Educational Research Association, New Orleans.

Friedman, B. (1989, March). Social reasoning about computer hacking, electronic information, and privacy in adolescence. Paper presented at the meeting of the American Educational Research Association, San Francisco.

Friedman, B. (1989, November). The school use of computer technologies to promote moral and social development. Paper presented to the meeting of the Association for Moral Education, Newport Beach, CA.

Kates, W. (1990, January 18). Morris testifies he wanted to produce a controllable computer 'worm.' Associated Press.

Kohlberg, L. (1980). High school democracy and educating for a just community. In R. Mosher (Ed.), Moral education: A first generation of research (pp. 20-57). New York: Praeger.

Kohlberg, L. (1985). The just community approach to moral education in theory and practice. In M. W. Berkowitz & F. Oser (Eds.), Moral education: Theory and application. Hillsdale, NJ: Lawrence Erlbaum.

Milgram, S. (1974). Obedience to authority. New York: Harper & Row.

Parker, D. B. (1984, December). The malicious computer hacker problem. Washington, DC: United States Department of Justice, Bureau of Justice Statistics.

Snapper, J. W. (1985). Responsibility for computer-based errors. Metaphilosophy, 16, 289-295.

Taylor, J. (1986, January 14). The copy-protection wars. PC Magazine, pp. 165-182.

Turiel, E. (1983). The development of social knowledge: Morality and convention. Cambridge: Cambridge University Press.